Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

30 821 Nationale Veiligheid

Nr. 116 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 17 september 2020

Afgelopen dagen berichtten diverse media over de opname van «sleutelfiguren» in een databestand van het Chinese databedrijf Zhenhua. Tijdens het Algemeen Overleg Raad Buitenlandse Zaken van 14 september jl. zegde de Minister van Buitenlandse Zaken toe om schriftelijk terug te komen op deze casus. Mede namens de ministers van Buitenlandse Zaken en Binnenlandse Zaken en Koninkrijksrelaties informeer ik u hierover. In diezelfde berichtgeving staat dat het gaat om het verzamelen van gegevens over personen wereldwijd, waaronder gegevens van Nederlanders en dat er op basis van de Nederlandse dataset geen aanwijzingen zijn dat gebruik zou zijn gemaakt van niet-openbare bronnen.

Deze mediaberichten passen in het beeld van de dreiging die uitgaat van statelijke actoren, zoals geschetst aan uw Kamer in onder andere de cybersecuritybeelden van de afgelopen jaren, de jaarverslagen van de inlichtingen- en veiligheidsdiensten, de Geïntegreerde Buitenland- en Veiligheidsstrategie, de aanpak rondom het tegengaan van statelijke dreigingen en de uitvoering van de Nederlandse Cybersecurity Agenda[1]. Het kabinet neemt deze dreiging uiterst serieus.

Er zijn statelijke actoren die op grote schaal persoonsgegevens verzamelen, zowel uit open bronnen, zoals op basis van contacten die iemand onderhoudt op sociale media, als uit niet-openbare bronnen, bijvoorbeeld door het hacken van hotelketens, telecombedrijven en medische instellingen. Ten aanzien van het verzamelen van openbare informatie geldt dat het op zichzelf niet verboden is, maar wel onwenselijk als deze informatie gebruikt wordt voor heimelijke of ondermijnende doeleinden. Ten aanzien van het verzamelen van niet-openbare informatie is de situatie anders, voor het verkrijgen van deze gegevens worden vaak onwettige methodes gebruikt.
De afgelopen jaren hebben de inlichtingen- en veiligheidsdiensten meermaals in onder meer jaarverslagen gemeld dat statelijke actoren

[1] Kamerstuk 26 643, nr. 614; Kamerstuk 26 643, nr. 647; Kamerstuk 30 821, nr. 72.

kst-30821-116
ISSN 0921 - 7371
's-Gravenhage 2020

gegevens verzamelen die voor hen op velerlei manieren van nut kunnen zijn, waaronder voor doeleinden die andere personen, organisaties of landen schaden. Voorbeelden hiervan zijn politieke en economische spionage, beïnvloeding van diaspora of het uitvoeren van digitale aanvallen (bijvoorbeeld *phishing*). Daarbij kan (vertrouwelijke) informatie van bijvoorbeeld ambtenaren, wetenschappers, topfunctionarissen en journalisten gericht worden gebruikt.

Weerbaarheid tegen statelijke dreigingen is daarom van groot belang. Het kabinet zet zich, zoals gemeld in de Kamerbrief tegengaan statelijke dreigingen, daarvoor in op het terrein van het tegengaan van ongewenste buitenlandse inmenging via diaspora, het beschermen van democratische instituties en processen en het versterken van de economische veiligheid. Daarnaast wordt er via de uitvoering van de Nederlandse Cybersecurity Agenda structureel ingezet op het verhogen van de digitale weerbaarheid van Nederland. Eerdergenoemde berichtgeving toont aan dat bewustwording bij personen en organisaties voor digitale veiligheid een essentieel onderdeel vormt van deze aanpak. Het kabinet zet zich daarom ook onverminderd in voor onder andere tijdige detectie en optimalisering van cyber- weerbaarheid van de Nederlandse samenleving en specifiek ten aanzien van instellingen die dergelijke data verzamelen.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus